

REMARKS

Favorable reconsideration of this application in light of the following discussion is respectfully requested.

Claims 20-38 are presently active in this case. Claims 1-19 were cancelled by a preliminary amendment. The present Amendment amends Claims 20, 30, and 32-33 without introducing any new matter.

The July 14, 2010 Office Action rejected Claims 20, 30 and 32-33 under 35 U.S.C. § 112, second paragraph, as being indefinite; and Claims 20-38 were rejected under 35 U.S.C. § 102(e) as anticipated by Harada et al. (U.S. Pat. App. Publ. No. 2003/0007640, now U.S. Pat. No. 7,698,571, hereinafter "Harada").

In response to the rejection of Claims 30 and 32 under 35 U.S.C. § 112, second paragraph, these claims are amended to recite that the scrambling platform and the descrambling platform are configured to perform certain features, to recite structural features of the respective platforms. It is believed that the terminology "configured to" clearly sets forth a structural limitation of the claimed element. As an example, an image pickup apparatus that picks up an image must inherently be *configured to* pick up an image, and thereby defines the structural features of the image pickup apparatus. Accordingly, it is respectfully submitted that the rejection under 35 U.S.C. § 112, second paragraph, is addressed.

Moreover, independent Claim 20 is amended to better comply with U.S. claim drafting practice. No new matter has been added.

In response to the rejection of independent Claim 20 under 35 U.S.C. § 102(e), Applicants respectfully request reconsideration of this rejection and traverse the rejection, as discussed next.

Briefly summarizing, Applicants' independent Claim 20 is directed to a method for securing scrambled data supplied to a plurality of receiver terminals, each of the terminals including a plurality of descrambling modules, each having a *specific processing capacity* and a *specific level of security*, the data being previously subdivided into M families, each comprising N blocks. The method includes the steps of scrambling, at a transmission, each block of a family by a key associated with the family, the key defined as a function of a specific processing capacity and a level of security of the respective deciphering modules; and descrambling, at a reception, each block of a family by the key associated with the family.

Turning now to the applied reference, Harada is directed to a system having a mobile phone 300 with a reception unit that receives a digital work from an external distribution server 200, an internal storage area 303 for storing the digital work, a playback unit 304 that plays back the digital work, and a unique information storage area 310 for storing information that is unique to the main device. (Harada, Abstract, Figs. 1, 3.) Moreover, in Harada's mobile phone 300, an encryption unit 320 encrypts the digital work using the unique information, and a decryption unit 340 decrypts, using the unique information, the encrypted digital work having been read from the recording medium device 400. (Harada, Fig. 3, Abstract, ¶¶ [0091], [0119], [0128].) In addition, Harada's write unit 330 writes the encrypted digital work into the removable recording medium device 400; and also has a read unit 350 that reads the encrypted digital work from the recording medium device 400. (Harada, Fig. 3, ¶ [0147]).

However, Harada fails to teach a step of "scrambling, at a transmission, each block of a family by a key associated with the family, defined as a function of a specific processing capacity and a level of security of the respective deciphering modules," as required by Applicants' independent Claim 20. The pending Office Action rejected this step of the

method of Applicants' Claim 20 by pointing to paragraph [0192] of Harada. In this paragraph, Harada explains that the encryption unit 320 or the decryption unit 340 of cell phone 300 can employ a Data Encryption Standard (DES) algorithm. (Harada, ¶¶ [0185]-[0192]). In particular, Harada states the following in this paragraph:

. . . at the time of encrypting the content using the DES encryption algorithm, the content is divided into data blocks each having 64 bits, and then each data block is encrypted using the 56-bit unique key to generate a 64-bit encrypted data block. The thus generated encrypted data blocks are then concatenated together, and the concatenated encrypted data blocks are outputted as the encrypted content (ECB (Electronic Codebook) mode). Alternatively, the encryption may be done using CBC (Cipher Feedback Changing) mode.

(Harada, ¶ [0192], ll. 1-11.) In other words, Harada solely describes that the encryption of each data block is performed by using a 56-bit unique key, but it is clear from the above-quoted passages of Harada that the key is *not* "defined as a function of a specific processing capacity and a level of security of the respective deciphering modules," as required by Applicants' independent Claim 20.

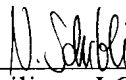
Therefore, the applied reference Harada fails to teach every feature recited in Applicants' Claim 20, so that Claims 20-29 are believed to be patentably distinct over Harada. Accordingly, Applicants respectfully traverse, and request reconsideration of the rejection based on this reference.

Consequently, in view of the present amendment, no further issues are believed to be outstanding in the present application, and the present application is believed to be in condition for formal Allowance. A Notice of Allowance for Claims 20-38 is earnestly solicited.

Should the Examiner deem that any further action is necessary to place this application in even better form for allowance, the Examiner is encouraged to contact Applicants' undersigned representative at the below listed telephone number.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, L.L.P.



Philippe J.C. Signore, Ph.D.
Attorney of Record
Registration No. 43,922

Customer Number

22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 07/09)

Nikolaus P. Schibli, Ph.D.
Registration No. 56,994